

INFORMATION \Leftarrow SECURITY

Lesson 1: Threats

Lesson 2: Protection

Lesson 3: Policies

Lesson 4: Security
Audits

Lesson 5: Tools &
Techniques

INFORMATION

SECURITY

Protection Mechanisms



GnuPG

Digital Signining
File Encryption

TrueCrypt

Disk Encryption

OpenSSL

Tunnel Encryption

OpenSSH

File Transfer Encryption

SandboxIE

Application Isolation

Little Snitch
Zone-Alarm

Personal Firewall

INFORMATION

SECURITY

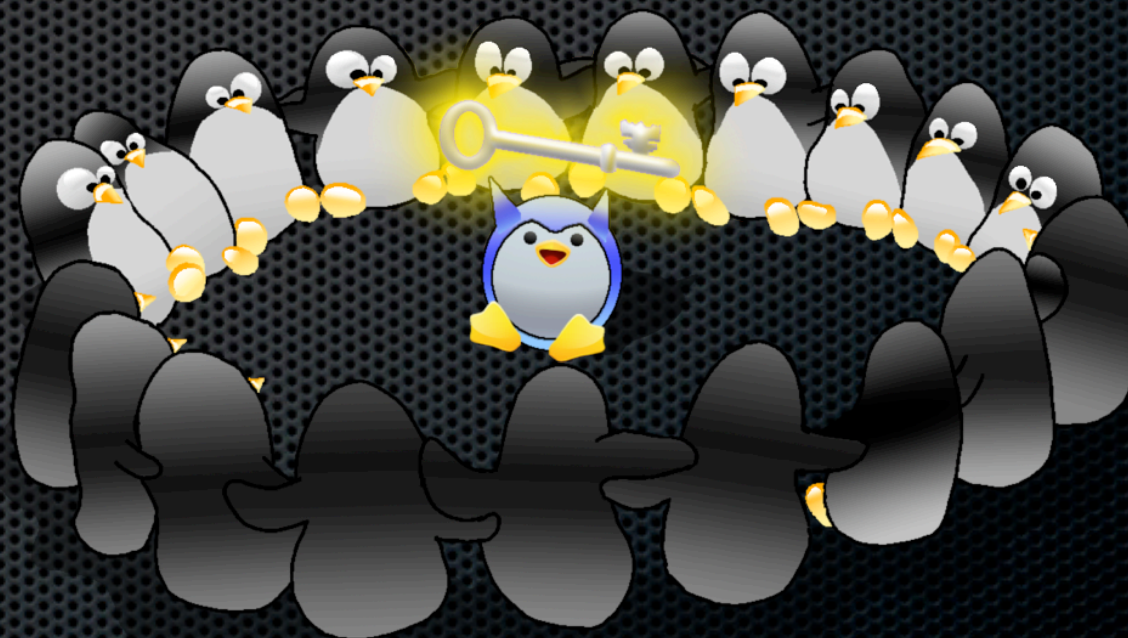
Cryptography

Keys

Public	Private
distributable	secret
paint on walls	keep under your pillow

Key Signing

- Generated Key
- Signed by a *trusted* authority



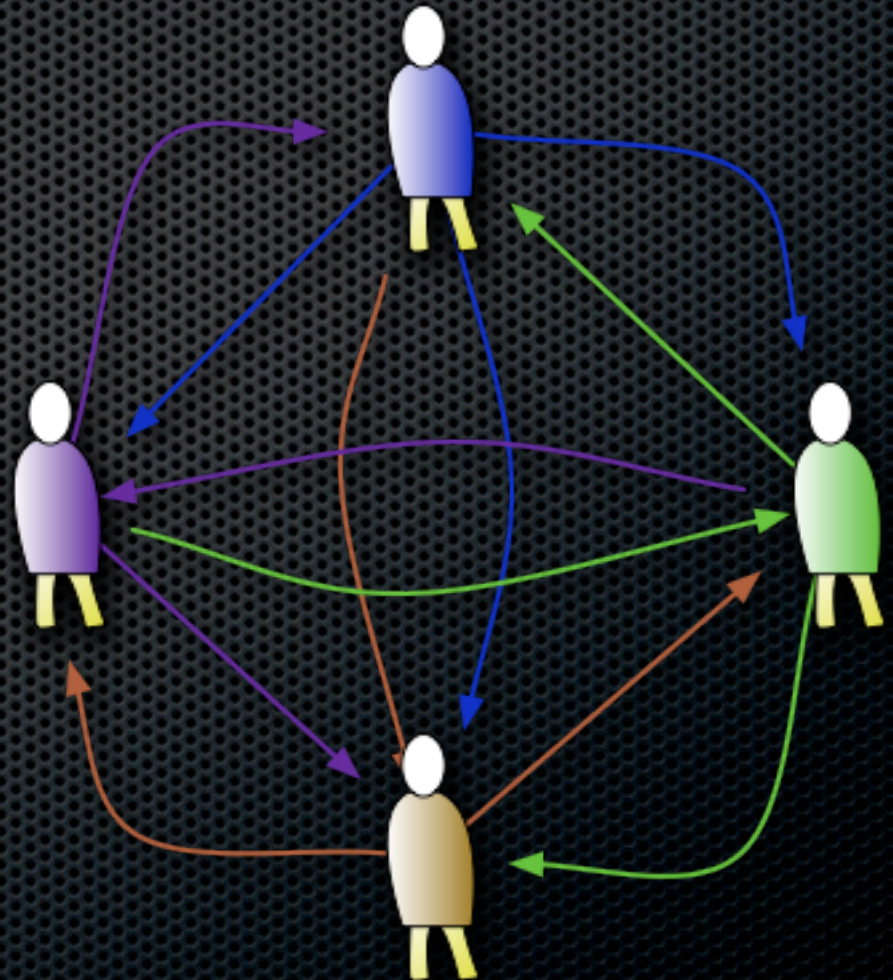
A key is bogus unless somebody vouches for it.

INFORMATION

SECURITY

Cryptography

Web of Trust

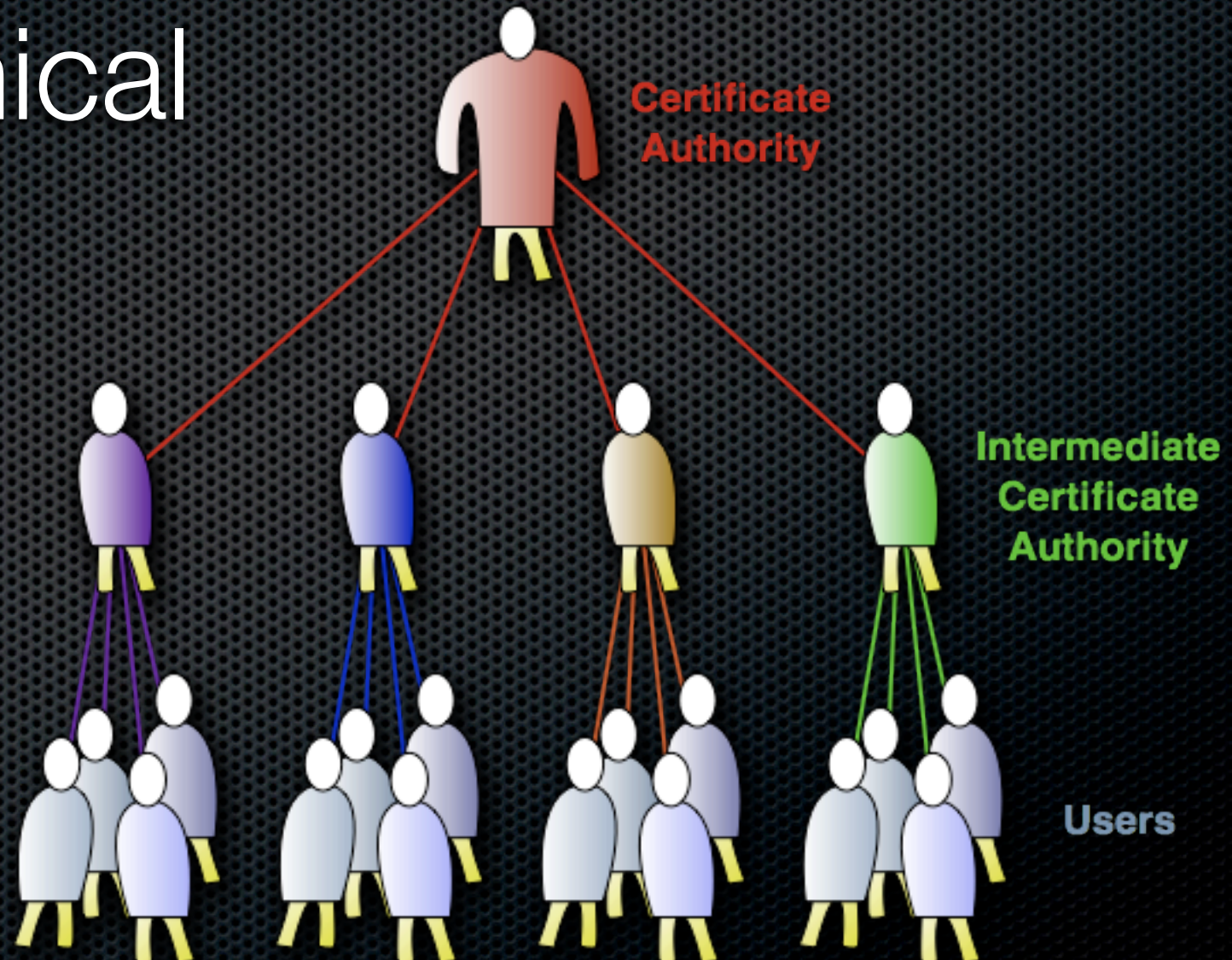


INFORMATION

SECURITY

Cryptography

Heirarchical



Key Strength

Symmetric Ciphers

Hash Method	Bits	Rounds
DES	56	16
3DES	168	48 (<i>DES equivalent</i>)
AES	128/256	10/14
MD5	128	64
SHA1	512	80

Key Strength

Asymmetric Ciphers

Hash Method	Bits	Equivalence
RSA	1,024	<i>80-bit symmetric</i>
RSA	2,048	<i>112-bit symmetric</i>
RSA	3,072	<i>128-bit symmetric</i>
RSA	15,360	<i>256-bit symmetric</i>

Salt

- Consider the MD5 Hash

i like kittens = 5ea27f3618bd7608a4edc07e7fd90315

- Virtual un-reversable
- Easily guessed with a rainbow table.
- Add a salt

i like kittens = c1ba200bd76bb6359bcd612d0658a3e

+ ball of string

- un-reversable
- un-guessable

Public Key Encryption

- Message encrypted with a public key can only be decrypted by the private key holder.

Encrypt	Decrypt
public key	private key

Private Key Signing

- Message signed with a private key can be verified by anybody with the public key.

Sign	Verify
private key	public key

Key-Pair Authentication

- Private key pair used for authentication.
- Only one public key for every private key.

Padlock <i>(on server)</i>	Key <i>(on client)</i>
public key	private key

Encrypted Tunnels

SSL / TLS

- Server gives its public key to clients.
- Client adds a salt to the public key and sends encrypted results to server.

Server	Client
private key + <i>client salt</i>	public key + <i>salt</i>

INFORMATION

SECURITY

Digital Signatures

GnuPG



INFORMATION

SECURITY

File Encryption

GnuPG



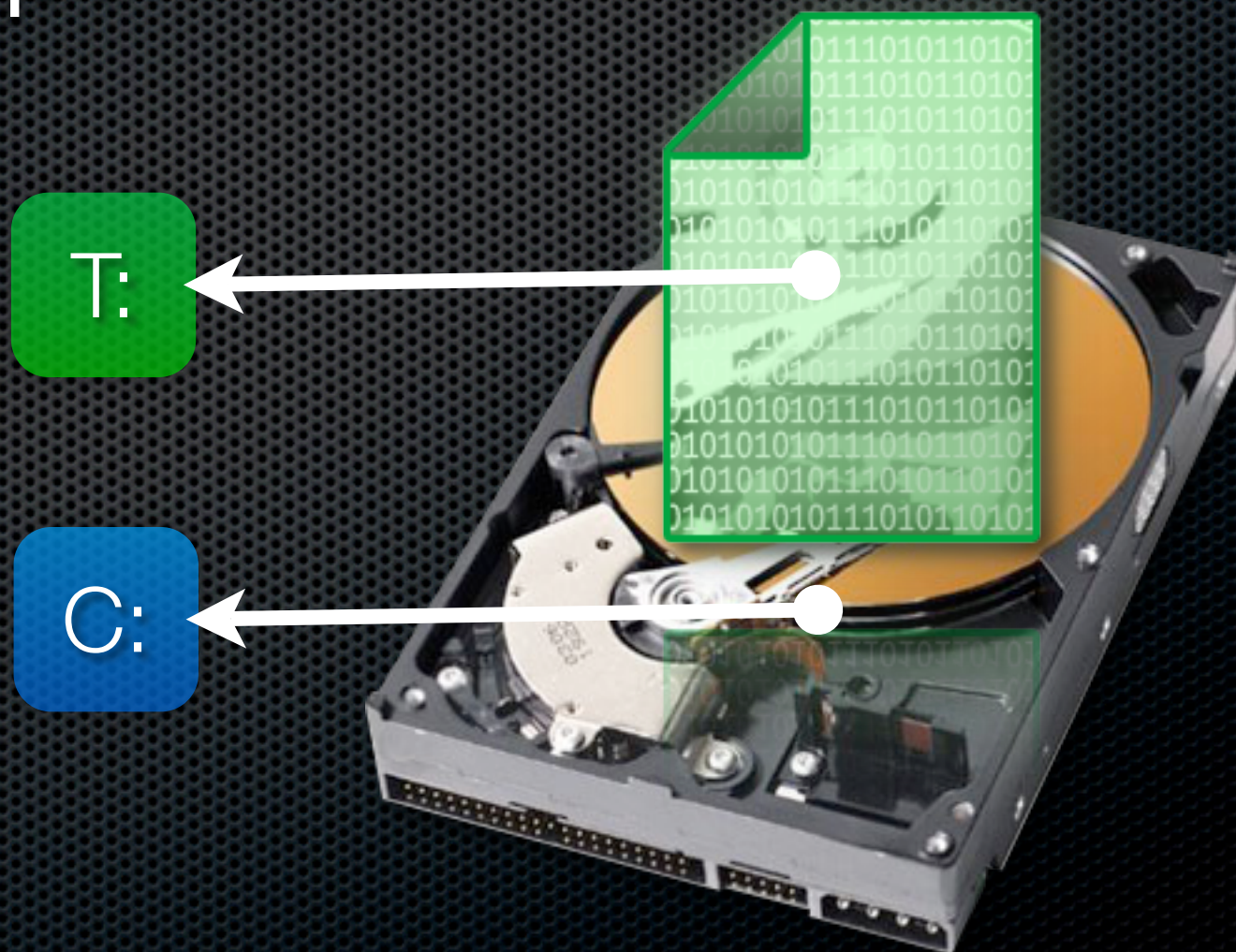
INFORMATION

SECURITY

Disk Encryption

True Crypt

Virtual Drives



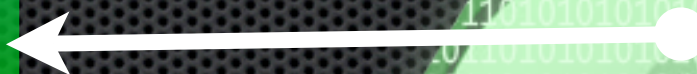
INFORMATION

SECURITY

Disk Encryption

True Crypt

Whole Disk Encryption



INFORMATION

SECURITY

Tunnel Encryption

OpenSSL



HTTPS

HTTP wrapped in an SSL tunnel

FTPS

FTP wrapped in an SSL tunnel

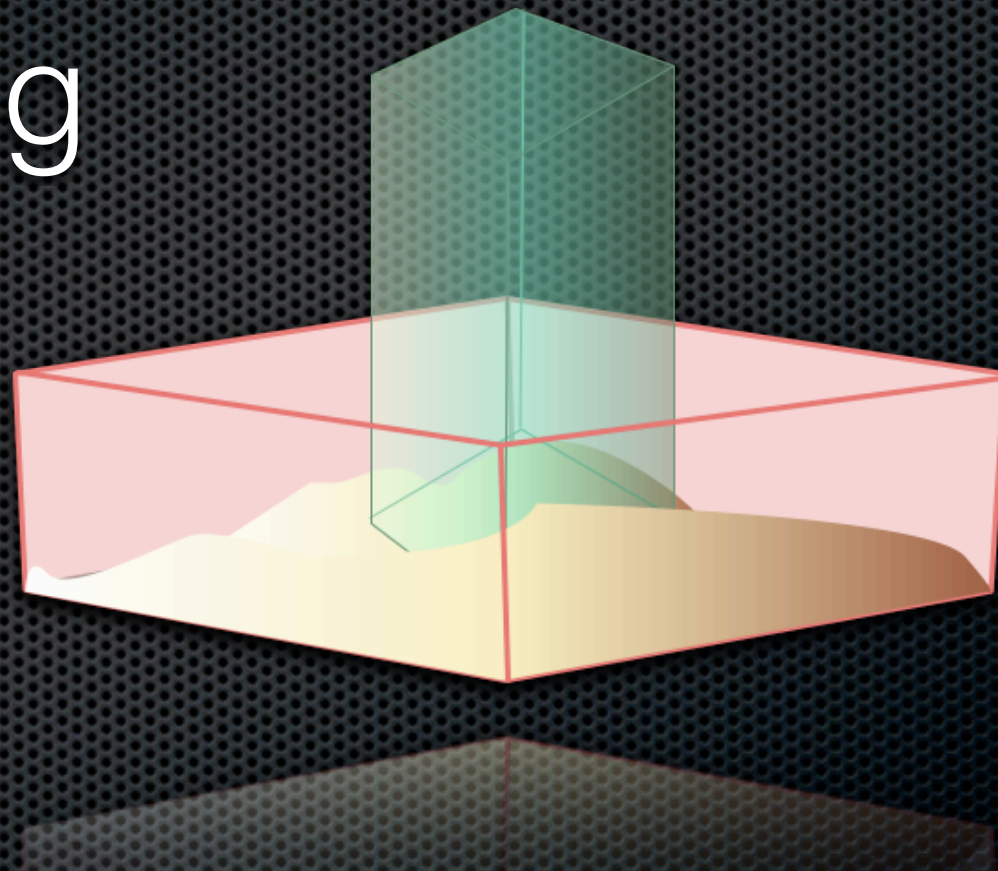
INFORMATION SECURITY

Transfer Encryption

OpenSSH

SSH	Secure Shell	<i>Replaces Telnet</i>
SCP	Secure Copy	<i>Alternative to FTP</i>
SFTP	Secure File Transfer Protocol	<i>Replaces FTP</i>

Sand Boxing

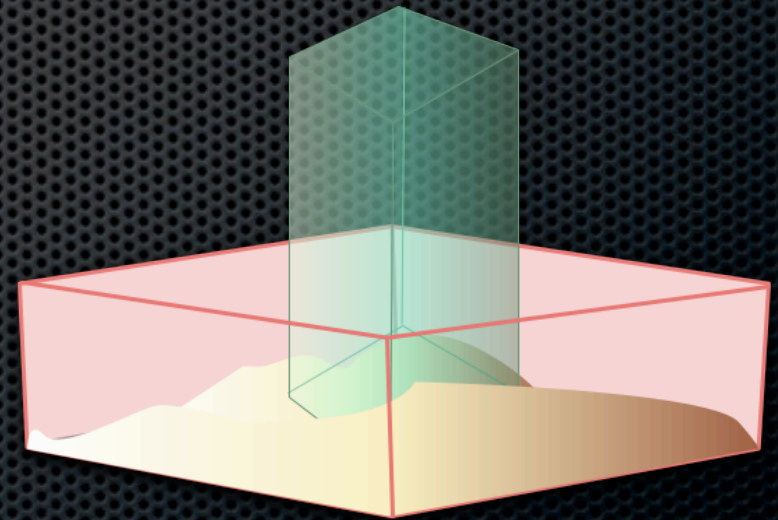
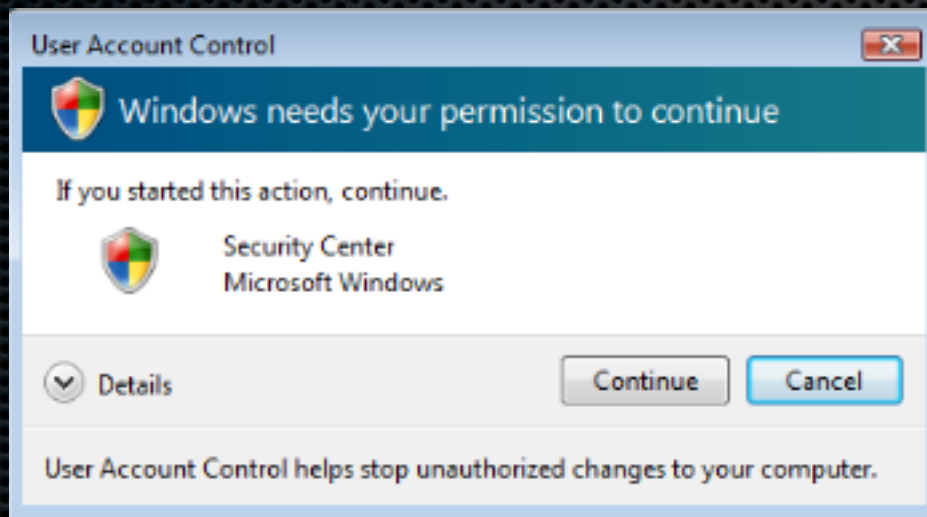


A sand box is a quasi-virtual environment. The application believes it has full system access, but in reality it can't step outside its sand box.

INFORMATION SECURITY

Application Isolation

ACL's are not Sandboxing



Access Control Lists determine what applications may have access to

INFORMATION SECURITY

Application Isolation



- Developed with IE in mind
- Can be used with any Application

Video
goes here

INFORMATION

SECURITY

Personal Firewall

ZoneAlarm



Little Snitch

INFORMATION

SECURITY

Personal Firewall

ZoneAlarm



Little Snitch

Songbird

wants to connect to **bundles.songbirdnest.com** on TCP port 80 (http). [Show Details...](#)

Once

Until Quit

Forever

- ☐ Any Connection
- ☒ → Port 80 TCP (http)
- ☐ → bundles.songbirdnest.com
- ☐ → bundles.songbirdnest.com & Port 80 TCP (http)

Deny

Allow

INFORMATION

SECURITY

Personal Firewall

ZoneAlarm



Little Snitch

Video
goes here

What *does* connect to the Internet
when you aren't looking ?

INFORMATION

SECURITY

Personal Firewall

ZoneAlarm



Little Snitch

INFORMATION

SECURITY

Personal Firewall

Zone-AAlarm



Little Snitch

Video
goes here

Is the Windows built-in Firewall enough ?